**IN THE UNITED STATES DISTRICT COURT**
**FOR THE WESTERN DISTRICT OF MISSOURI**
**SOUTHERN DIVISION**

| | |
|---|---|
| **IN THE MATTER OF THE SEARCH OF:**<br><br>**A MOTOROLA CELLULAR TELEPHONE, MODEL NUMBER XT2052DL, IMEI: 351638116135718**<br><br>**CURRENTLY LOCATED AT THE JOPLIN, MISSOURI, POLICE DEPARTMENT, 303 EAST 3RD STREET, JOPLIN, MISSOURI** | **Case No. 21-SW-2156DPR** |

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE**

I, Lee Walker, a Task Force Officer (TFO) with the Federal Bureau of Investigation (FBI), being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I have been employed as a police officer with the City of Springfield, Missouri, since November 2004. I am currently a TFO with the FBI, as well as a member of the Southwest Missouri Cyber Crimes Task Force (SMCCTF) in Joplin, Missouri. As a TFO, I have been assigned to investigate computer crimes, including violations against children. I have gained expertise in the conduct of such investigations through training in seminars, classes, and everyday work related to conducting these types of investigations. I have attended training provided by the FBI Cyber Crime Division, the FBI's Regional Computer Forensic Laboratory, and the Missouri Internet Crimes Against Children (ICAC) Task Force. I have written, executed, and assisted in over 100 search warrants on the state and federal level. As a TFO with the FBI, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. I have received training in the area of child pornography and child

exploitation and have reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media.

2. As part of this affiant's duties with FBI, this affiant investigates criminal violations relating to the production, receipt, possession, and distribution of child pornography, in violation of 18 U.S.C. §§ 2251, 2252, and 2252A, and the production, distribution, receipt, or possession with intent to distribute obscene visual representations of the sexual abuse of children in violation of 18 U.S.C. § 1466A.

3. The statements in this affidavit are based on my personal observations, training and experience, investigation of this matter, and information obtained from other agents and witnesses. Because this affidavit is being submitted for the limited purpose of securing a search warrant, this affiant has not included each and every fact known to me concerning this investigation.

## IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. This affiant has set forth the facts necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 1466A, 2251, 2252, and 2252A, are contained within the following electronic device - **a Motorola cellular phone, model number XT2052DL, IMEI: 351638116135718** (hereinafter, also referred to as "the Device"), which was surrendered to FBI TFO Charles "Chip" Root by the Executive Director of Alpha House on September 14, 2021. The Device is currently stored at the Joplin, Missouri, Police Department (JPD), located at 303 East 3rd Street, Joplin, Jasper County, Missouri, also within the Western District of Missouri.

5. This affidavit is in support of an application for a search warrant for evidence, fruits, and instrumentalities of the foregoing criminal violations, which relate to the knowing possession, receipt, distribution, and/or production of child pornography, and the knowing

production, distribution, receipt, and/or possession with intent to distribute obscene visual representations of the sexual abuse of children. The property to be searched is described in the following paragraphs and fully in Attachment A. This affiant requests the authority to search and/or examine the seized items, specified in Attachment B, as instrumentalities, fruits, and evidence of crime.

6. The applied-for warrant would authorize the forensic examination of the device for the purpose of identifying electronically stored data particularly described in Attachment B.

7. This affiant has probable cause to believe that evidence of violations of 18 U.S.C. §§ 1466A, 2251, 2252, and 2252A, involving the use of a computer, in or affecting interstate commerce, to produce, distribute, receive, and/or to possess with intent to distribute obscene visual representations of the sexual abuse of children and/or to produce, receive, possess, and/or distribute child pornography, are located in and within the aforementioned property described below. Thus, as outlined below, and based on my training and experience, there is probable cause to believe that evidence, fruits, and/or instrumentalities of the aforementioned crimes are located in this property.

## PROBABLE CAUSE

8. On September 8, 2021, Alpha House Executive Director (ED) Sue Marshall requested FBI assistance in conducting an investigation into a resident of Alpha House, identified as Brandon DEAVERS, and his involvement in possessing suspected images of child pornography. According to ED Marshall, on September 4, 2021, Alpha House Watch Officer (WO) Raya Doran, discovered DEAVERS sitting in a common area of the facility. DEAVERS appeared to be using a cellular telephone. WO Doran was aware that DEAVERS was prohibited from possessing an internet capable cellular telephone because DEAVERS was a sex offender. WO Doran confronted

DEAVERS and verified that DEAVERS was using an internet capable cellular telephone. WO Doran seized the device. While speaking with Doran, DEAVERS admitted that "cartoon" images of child pornography would be located on the device. DEAVERS also admitted to paying an unidentified co-worker to purchase a new cellular telephone for his use. The device seized from DEAVERS was identified as a **Motorola cellular phone, model number XT2052DL, IMEI: 351638116135718**. WO Doran turned the Device over to ED Marshall for storage.

18. After receiving the Device from WO Doran, ED Marshall viewed some of the contents on the device. She observed a cartoon image of a naked adult male, with his penis exposed to a child on DEAVERS's device. The image included the caption, "I thought Mom would never leave." ED Marshall referred the matter to the Federal Bureau of Prisons (BOP), as DEAVERS was in their custody, but housed at Alpha House at the time of the incident. BOP requested the matter be referred to the FBI for investigation.

19. DEAVERS was in the custody of BOP because he had been previously found guilty of receipt and distribution of child pornography. Specifically, on or about May 15, 2017, DEAVERS pled guilty to one count of receipt and distribution of child pornography in the United States Court for the Western District of Missouri, in Case No. 17-04006-01-CR-C-SRB. On February 22, 2018, DEAVERS was sentenced to 72 months in BOP followed by a 20-year term of supervised release.

20. Alpha House is a residential reentry center for federal offenders, who have been released from federal prison. It is located at 2300 East Division Street, Springfield, Missouri 65803, located within the Western District of Missouri.

22. On September 14, 2021, FBI TFO Root contacted ED Marshall at the facility. ED Marshall provided the TFO Root with DEAVERS's cellular telephone, and the related Alpha

House documentation of the incident. ED Marshall identified the unlock pattern to DEAVER's device as a "Z." The Device was transported to the Joplin Police Department, located at 303 East 3rd Street, Joplin, Missouri for storage, pending the receipt of a search warrant.

23. Due to the above information, I believe that the Device contains information related to the production, distribution, receipt, and possession with intent to distribute obscene visual representations of the sexual abuse of children and the production, receipt, distribution, and possession of child pornography and evidence of violations of 18 U.S.C. §§ 1466A, 2251, 2252, and 2252A.

## TECHNICAL TERMS

24. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Computer: The term "computer" as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

b. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities

include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

c. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

d. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

e. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

f. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments. or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

g. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

h. Pager: A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.

i. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

j. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

18. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, computer, digital camera, portable media player, GPS, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

## ELECTRONIC STORAGE AND FORENSIC ANALYSIS

25. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

26. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition,

a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

27. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

28. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

29. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

## CONCLUSION

30. Based on the above facts, this affiant believes probable cause exists for the issuance of a warrant to search the Device described more fully in Attachment A for (1) property that constitutes evidence of the commission of a criminal offense; (2) contraband, the fruits of a crime, or things otherwise criminally possessed; and/or (3) property designated or intended for use or which is or has been used as the means of committing a criminal offense, namely possible violations of 18 U.S.C. §§ 1466A, 2251, 2252, and 2252A, including, but not limited to, the items listed in Attachment B.

Further Affiant Sayeth Naught.

Lee Walker
Task Force Officer
Federal Bureau of Investigation

Subscribed and sworn to before me via telephone on the 4th day of November 2021.

HONORABLE DAVID P. RUSH
Chief United States Magistrate Judge
Western District of Missouri